Um provedor de identidades para autenticação de dispositivos e de usuários baseado no padrão SAML*

Marlon Cordeiro Domenech[1,2]†, Gabriel Massuqueti de Carvalho[2], Michelle Silva Wangham[1,2]

[1]Laboratório de Sistemas Embarcados e Distribuídos
Universidade do Vale do Itajaí (UNIVALI) – Itajaí, SC – Brasil

[2]4 Vision Lab
Universidade do Vale do Itajaí (UNIVALI) – São José, SC – Brasil

{marloncdomenech, gabrielcarvalho}@edu.univali.br, wangham@univali.br

Abstract. *Internet of Things (IoT) covers a hardware, software and services infrastructure able to connect things to Internet. Things and users need authentication for secure communication. Support for different authentication mechanisms for users and devices in the same infrastructure is an open problem in the context of IoT. This paper describes an SAML Identity Provider able to authenticate users and devices. After authentication, IdP issues short-lived tokens in a portable and interoperable manner (SAML tokens).*

1. Introdução

A Internet das Coisas (*Internet of Things* – IoT) abrange uma infraestrutura de hardware, software e serviços que conectam objetos físicos, como carros, dispositivos médicos e máquinas industriais à rede de computadores, permitindo que os objetos interajam e cooperem entre si afim de atingir um objetivo comum. A IoT apresenta características como restrições de recursos computacionais e de energia. Neste cenário, as questões de segurança requerem abordagens diferenciadas das adotadas nos ambientes computacionais tradicionais [Atzori et al. 2010].

Os dispositivos da IoT podem utilizar mecanismos de autenticação diferentes daqueles utilizados por usuários humanos. Logo, é preciso prover uma infraestrutura que suporte diferentes mecanismos de autenticação de dispositivos e de usuários. Esse suporte é abordado na literatura para usuários, em [Akram e Hoffmann 2008] e [Conzon et al. 2012]. Contudo, ainda é um problema em aberto para dispositivos da IoT.

Este trabalho descreve um Provedor de Identidades (*Identity Provider* - IdP) baseado na especificação SAML (*Security Assertion Markup Language*), capaz de autenticar usuários e dispositivos que utilizam diferentes mecanismos de autenticação. Após a autenticação, o IdP gera *tokens* de vida curta, os quais são aceitos por entidades que confiam no IdP e das quais o usuário ou dispositivo deseja consumir um recurso.

2. Abordagem Proposta

A especificação SAML 2.0 define um padrão de representação e troca de informações de segurança entre componentes de um sistema distribuído. Por ser um padrão, o uso do

*Projeto financiado pelo CNPq (RHAE 459623/2013-3) e pela Microsoft Research (”PaaS for smart machines monitoring and control”).

†Bolsista CAPES.

SAML favorece a interoperabilidade entre sistemas. O SAML provê suporte nativo a mecanismos para autenticação de dispositivos e de usuários, além de pontos de extensão que permitem a inclusão de outros mecanismos de autenticação, sem perda de interoperabilidade. Mensagens SAML podem ser transportadas utilizando mensagens HTTP padrão, o que viabiliza o uso da especificação em contextos com usuários e dispositivos. Por fim, o SAML é a solução mais adotada em sistemas de gestão de identidades que seguem o modelo federado e proveem autenticação única (*Single Sign On*) federada. Nos sistemas de identidades federadas, um usuário autenticado em seu IdP pode acessar serviços (SPs) de outros domínios administrativos sem precisar se autenticar novamente. É necessário que IdPs e SPs destes domínios administrativos estabeleçam relações de confiança.

A solução proposta é composta de três partes: (i) os metadados das identidades; (ii) uma aplicação de registro de usuários e dispositivos no IdP; e (iii) mecanismos de autenticação no IdP. Os metadados dos usuários são compostos dos atributos nome, sobrenome, e-mail, organização, unidade organizacional, função, cpf (identificador único) e certificado digital. Já os metadados dos dispositivos tiveram como base os atributos utilizados para descrever dispositivos em plataformas de Cloud com foco em IoT[1]. Os atributos dos dispositivos são o número de série (identificador único), nome de exibição, contato do administrador, organização, unidade organizacional, descrição, tipo de dispositivo, referência de localização física (latitude, longitude, altitude), disposição (fixo ou móvel), exposição (*indoor* ou *outdoor*) e status (*online* ou *offline*). Estes metadados são definidos em um XML Schema que padroniza a representação e processamento pelas entidades que consomem os *tokens* de segurança gerados pelo IdP, contendo tais atributos.

A aplicação de registro de dispositivos e de usuários é utilizada pelo administrador do IdP para cadastrar, recuperar, atualizar e excluir registros. Para prova de conceito, o IdP proposto autentica usuários usando certificados digitais no formato X.509 e dispositivos usando o acordo de chaves autenticado não-interativo Sakai-Ohgishi-Kasahara [Sakai et al. 2000], que é um criptossistema baseado em identidades, que utiliza um parâmetro público da identidade da entidade para calcular sua chave pública.

Assim, ao cadastrar um usuário, o administrador deverá informar ao IdP os dados da identidade deste e inserir o certificado digital que será utilizado na etapa de autenticação. Ao registrar um dispositivo, este deve estar conectado fisicamente ao IdP. O administrador deverá inserir as informações de identidade do dispositivo e, com base no número de série e na chave mestra (única, conhecida apenas pelo IdP e gerada antecipadamente), o IdP calcula uma chave privada para o dispositivo. Em seguida, o arquivo com a chave privada é transferido para o dispositivo, para utilização na etapa de autenticação.

O processo de autenticação do cliente ocorre conforme descrito a seguir e utiliza apenas mensagens HTTP sobre um canal SSL , em que o IdP é autenticado:

1. O cliente envia uma requisição de autenticação SAML para um *endpoint* do IdP e recebe como resposta o redirecionamento para o *endpoint* de escolha de mecanismo de autenticação;
2. O cliente segue o redirecionamento. Em seguida, envia uma mensagem HTTP GET para o *endpoint* de escolha do mecanismo de autenticação, indicando na URL (via Query String) o mecanismo de autenticação escolhido;

[1]Foram utilizadas como base as plataformas DeviceHive, Xively, Thingworx, Evrything e Axeda.

3. É iniciada a etapa de autenticação. Caso seja um usuário, o certificado digital é solicitado pelo IdP e enviado pela aplicação cliente. Para que seja autenticado, o campo *CN* do certificado deverá ser igual ao campo *uid* da identidade do usuário armazenada no IdP, além do certificado digital ser igual ao certificado cadastrado na etapa de registro. Caso seja um dispositivo, o IdP executa o protocolo de *challenge-response* descrito em [Needham e Schroeder 1978]. O IdP calcula um *challenge* (criptografado com o algoritmo AES_256, em que a chave é uma chave de sessão calculada com base na identidade do dispositivo e na identidade e chave privada do IdP) e envia ao dispositivo, que calcula o respectivo *response* (com base na identidade do IdP e identidade e chave privada do dispositivo);
4. Caso a autenticação seja bem sucedida, o IdP envia ao cliente uma mensagem *SAML Response* contendo a asserção SAML solicitada, ambas assinadas digitalmente. A asserção SAML atesta que o cliente se autenticou e pode conter os atributos da identidade deste cliente.

3. Considerações Finais

A aplicação de registro foi desenvolvida em PHP 5 e utiliza o OpenLDAP como serviço de diretório para armazenamento das identidades. O IdP SAML foi implementado com base no framework SimpleSAMLphp. As extensões para utilização do mecanismo de autenticação de dispositivos foram definidas e implementadas, visando preservar a conformidade do IdP com a especificação SAML. Os próximos passos são: (i) executar testes de software para avaliar o atendimento aos requisitos definidos na solução proposta; e (ii) avaliar o uso de recursos computacionais do cliente, visando avaliar a viabilidade da proposta em cenários com clientes computacionalmente restritos. Neste teste, será utilizado um BeagleBone Black[2] como dispositivo cliente. As métricas utilizadas serão o tamanho das mensagens, tempo de processamento, uso de memória RAM e flash/disco, uso de CPU, impactos na vazão da rede e consumo de energia elétrica.

Referências

Akram, H. e Hoffmann, M. (2008). Supports for identity management in ambient environments-the hydra approach. In *Proceedings...*, pages 371–377. 3rd International Conference on Systems and Networks Communications, 2008. ICSNC'08.

Atzori, L., Iera, A., e Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787–2805.

Conzon, D., Bolognesi, T., Brizzi, P., Lotito, A., Tomasi, R., e Spirito, M. A. (2012). The virtus middleware: An xmpp based architecture for secure iot communications. In *Proceedings...*, pages 1–6. 21st International Conference on Computer Communications and Networks (ICCCN), 2012.

Needham, R. M. e Schroeder, M. D. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999.

Sakai, R., Ohgishi, K., e Kasahara, M. (2000). Cryptosystems based on pairing. In *The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan*, pages 135–148.

[2]http://beagleboard.org/black